This listing of claims will replace all prior versions, and listings, of claims in the application:

LISTING OF CLAIMS:

1. (Previously Presented) A method for accessing a multicast event comprising:

receiving a request for a ticket at a ticket server, said request being from a receiving client, wherein the receiving client is to participate in the multicast event transmitted by a sending client, receipt of said ticket to qualify the receiving client to access a key from a key server, wherein the key is a symmetric key that the sending client uses to encrypt the multicast event and the receiving client uses to decrypt the multicast event, said key to facilitate access to the multicast event by at least one receiving client;

determining if the receiving client is authorized to receive the key; and

transmitting the ticket from the ticket server to the receiving client if the receiving client is authorized.

2. (Previously Presented) The method of claim 1 wherein determining if the receiving client is authorized comprises:

accessing a database that defines authorized clients; and

determining if the receiving client is among the authorized clients defined by the database.

3. (Previously Presented) The method of claim 1 further comprising:

accessing a database that defines associations between authorized clients and multicast events;

constructing a summary of all multicast events to which the receiving client is associated based on the database; and

including the summary in the ticket.

4. (Previously Presented) The method of claim 3 wherein the database comprises a directed hierarchy of groups, wherein each group comprises at least one member client and/or at least one member event, and wherein constructing the summary comprises:

locating a particular group in the database to which the receiving client is a member client;

adding identifying information to the summary for each multicast event, if any, belonging to the particular group;

locating at least one ancestor group to the particular group in the directed hierarchy of groups; and

adding identifying information to the summary for each event, if any, belonging to the at least one ancestor group.

5. (Previously Presented) The method of claim 1 wherein the ticket comprises at least one of an identifier that indicates a group to which the receiving client belongs, a list identifying at least one multicast event for which the receiving client is qualified, and a digital certificate that indicates that the receiving client is authorized for each listed multicast event.

6. (Previously Presented) The method of claim 5 wherein the list comprises at least one of a title of each listed event, an internet protocol (IP) address for each listed event, a time indication for each listed event, and an IP address for a key server corresponding to each listed multicast event.

7. (Currently Amended) A method comprising:

receiving a request for a key at a key server, said request being received from a receiving client, ~~and~~ said key to facilitate access to ~~the~~ a multicast event by the receiving client, wherein the key is a symmetric key that ~~the~~ a sending client uses to encrypt the multicast event and the receiving client uses to decrypt the multicast event;

determining if the receiving client is qualified to receive the key based on a ticket previously obtained by the receiving client from a ticket server; and

transmitting the key from the key server to the receiving client if the receiving client is qualified.

8. (Previously Presented) The method of claim 7 wherein the key comprises at least one of an initiation time for use of the key and a lifetime for the key.

9. (Previously Canceled).

10. (Previously Presented) The method of claim 7 wherein the request comprises an initial request for the event, and wherein receiving the initial request comprises:

receiving the initial request at a particular time during a predetermined period before the multicast event, said particular time being randomly generated by the receiving or sending client.

11. (Previously Presented) The method of claim 7 further comprising:

establishing a secure point-to-point link between the key server and the receiving client in response to the requests, wherein the key is transmitted over the secure point-to-point link.

12. (Previously Presented) The method of claim 7 wherein the request comprises one of a plurality of refresh requests, wherein each of the plurality of refresh requests corresponds to one of a plurality of forward security windows during the multicast event, wherein each of the plurality of forward security windows comprises a repeated time interval, and wherein receiving the refresh request comprises:

receiving the refresh request at a particular time within a corresponding forward security window, said particular time being randomly generated by the receiving or sending client for a first forward security window and applied at the repeated time interval thereafter.

13. (Previously Presented) The method of claim 7 wherein the key corresponds to a first interval of the multicast event, and wherein the method further comprises:

determining if the receiving client remains qualified to receive a refresh key; and

transmitting the refresh key to the receiving client if the receiving client remains qualified, said refresh key corresponding to the subsequent interval of the multicast event.

14. (Previously Presented) The method of claim 7 wherein the key corresponds to a first interval of the multicast event, and wherein the method further comprises:

receiving a plurality of additional requests for the key from a plurality of additional receiving clients;

determining if each of the plurality of additional receiving clients are qualified to receive the key based on a ticket previously obtained by each of the plurality of additional receiving clients from the ticket server;

transmitting the key to each of the plurality of additional receiving clients that are qualified;

determining if the receiving client and each of the plurality of additional receiving clients remain qualified to receive a refresh key; and

transmitting the refresh key to the receiving client if the receiving client remains qualified and to each of the plurality of additional receiving clients that remain qualified, said refresh key corresponding to a subsequent interval of the multicast event.

15. (Previously Presented) The method of claim 14 further comprising:

establishing a secure multicast link from the key server to the receiving client and the plurality of additional receiving clients, wherein the refresh key is transmitted through the secure multicast link.

16. (Original) The method of claim 7 wherein the key server has a synchronized time with respect to a sending client for the event to within a margin of error, and wherein the method further comprises:

determining which of a plurality of available keys to use for said key based on the synchronized time.

17. (Previously Presented) The method of claim 7 wherein determining comprises at least one of:

verifying that the request is received within a predetermined period before the multicast event or time interval during the multicast event; and

verifying that the request includes credentials for the multicast event.

18. (Previously Presented) The method of claim 7 wherein the request is received within a predetermined time frame after the multicast event starts, wherein said multicast event is not encrypted during the predetermined time.

19. (Previously Presented) A machine readable storage medium having stored thereon machine executable instructions, execution of said machine executable instructions to implement a method comprising:

obtaining a ticket at a client from a ticket server, said ticket to facilitate access to a multicast event by the client;

obtaining a key at the client from a key server based on the ticket, wherein the key is a symmetric key used to encrypt the multicast event and used by the client to decrypt the event; and

participating in the multicast event based on the key.

20. (Previously Presented) The machine readable storage medium of claim 19 wherein obtaining the ticket comprises:

sending a request to the ticket server for a list of multicast events in which the client is qualified to participate.

21. (Previously Presented) The machine readable medium of claim 19 wherein obtaining the key comprises:

receiving an indication to participate in the multicast event; and

initiating a transaction with the key server at a location indicated by the ticket and within a time frame prior to a start time of the multicast event indicated by the ticket.

22. (Previously Presented) A machine readable storage medium having stored thereon machine executable instructions, the execution of said machine executable instructions to implement a method comprising:

receiving a request for a key at a key server, said request being received from a receiving client, and said key to facilitate an event between the receiving client and a sending client, wherein the key is a symmetric key that the sending client uses to encrypt the event and the receiving client uses to decrypt the event;

determining if the receiving client is qualified to receive the key based on a ticket previously obtained by the receiving client from a ticket server; and

transmitting the key from the key server to the receiving client if the receiving client is qualified.

23. (Previously Presented) The machine readable storage medium of claim 22 wherein the request comprises an initial request for the event, and wherein receiving the initial request comprises:

receiving the initial request at a particular time during a predetermined period before the event, said particular time being randomly generated by the receiving client.

24. (Previously Presented) The machine readable storage medium of claim 22

further comprising:

establishing a secure point-to-point link between the key server and the receiving client in response to the request, wherein the key is transmitted over the secure point-to-point link.

25 . (Previously Presented) The machine readable storage medium of claim 22 wherein the request comprises one of a plurality of refresh requests, wherein each of the plurality of refresh requests corresponds to one of a plurality of forward security windows during the event, wherein each of the plurality of forward security windows comprises a repeated time interval, and wherein receiving the refresh request comprises:

receiving the refresh request at a particular time within a corresponding forward security window, said particular time being randomly generated by the receiving or sending client for a first forward security window and applied at the repeated time interval thereafter.

26 . (Previously Presented) The machine readable storage medium of claim 22 wherein the key corresponds to a first interval of the event, and wherein the method further comprises:

determining if the receiving client remains qualified to receive a refresh key; and

transmitting the refresh key to the receiving client if the receiving client remains qualified, said refresh key corresponding to a subsequent interval of the event.

27. (Previously Presented) The machine readable storage medium of claim 22 wherein the key corresponds to a first interval of the event, and wherein the method further

comprises:

receiving a plurality of additional requests for the key from a plurality of additional receiving clients;

determining if the each of the plurality of additional receiving clients are qualified to receive the key based on a ticket previously obtained by each of the plurality of additional receiving clients from the ticket server;

transmitting the key to each of the plurality of additional receiving clients that are qualified;

determining if the receiving client and each of the plurality of additional receiving clients remain qualified to receive a refresh key; and

transmitting the refresh key to the receiving client if the receiving client remains qualified and to each of the plurality of additional receiving clients that remain qualified, said refresh key corresponding to a subsequent interval of the event.

28. (Previously Presented) The machine readable storage medium of claim 27 wherein the request is received within a predetermined time frame after the event starts, wherein said event is not encrypted during the predetermined period time frame.

29. (Currently Amended) A ticket server apparatus for facilitating access to a multicast event comprising:

a port to receive a request for a ticket, said request being from a receiving client, said ticket to qualify the receiving client to access a key from a key server, ~~said key to facilitate an event between the client and at least one additional client,~~ wherein the key is a symmetric key used by a sending client to encrypt the event and used by the receiving client to decrypt the event; and

circuitry to determine if the receiving client is authorized to receive the key, and to transmit the ticket through the port to the receiving client if the receiving client is authorized .

30. (Currently Amended) A key server apparatus for facilitating access to a multicast event comprising:

a port to receive a request for a key, said request being received from a receiving client, ~~and said key to facilitate an event between the client and at least one additional client,~~ wherein the key is a symmetric key used by a sending client to encrypt the event and used by the receiving client to decrypt the event; and

circuitry to determine if the receiving client is qualified to receive the key based on a ticket previously obtained by the receiving client from a ticket server, and to transmit the key through the port to the receiving client if the receiving client is qualified.

31. (New) A method for accessing a multicast event comprising:

receiving a request for a ticket at a ticket server, said request being from a receiving client, wherein the receiving client is to participate in the multicast event transmitted by a sending client, receipt of said ticket to qualify the receiving client to access a key from a key server, wherein the key is a symmetric key that the sending client uses to encrypt the multicast event and the receiving client uses to decrypt the multicast event, said key to facilitate access to the multicast event by at least one receiving client;

determining if the receiving client is authorized to receive the key;

transmitting the ticket from the ticket server to the receiving client if the receiving client is authorized;

accessing a database that defines associations between authorized clients

and multicast events;

constructing a summary of all multicast events to which the receiving client is associated based on the database; and

including the summary in the ticket;

wherein the database comprises a directed hierarchy of groups, wherein each group comprises at least one member client and/or at least one member event, and wherein constructing the summary comprises:

locating a particular group in the database to which the receiving client is a member client;

adding identifying information to the summary for each multicast event, if any, belonging to the particular group;

locating at least one ancestor group to the particular group in the directed hierarchy of groups; and

adding identifying information to the summary for each event, if any, belonging to the at least one ancestor group.

32. (New) A method for accessing a multicast event comprising:

receiving a request for a ticket at a ticket server, said request being from a receiving client, wherein the receiving client is to participate in the multicast event transmitted by a sending client, receipt of said ticket to qualify the receiving client to access a key from a key server, wherein the key is a symmetric key that the sending client uses to encrypt the multicast event and the receiving client uses to decrypt the multicast event, said key to facilitate access to the multicast event by at least one receiving client;

determining if the receiving client is authorized to receive the key; and

transmitting the ticket from the ticket server to the receiving client if the

receiving client is authorized;

wherein the ticket comprises at least one of an identifier that indicates a group to which the receiving client belongs, a list identifying at least one multicast event for which the receiving client is qualified, and a digital certificate that indicates that the receiving client is authorized for each listed multicast event.

33. (New) The method of claim 32 wherein the list comprises at least one of a title of each listed event, an internet protocol (IP) address for each listed event, a time indication for each listed event, and an IP address for a key server corresponding to each listed multicast event.

34. (New) A method comprising:

receiving a request for a key at a key server, said request being received from a receiving client, said key to facilitate access to a multicast event by the receiving client, wherein the key is a symmetric key that a sending client uses to encrypt the multicast event and the receiving client uses to decrypt the multicast event;

determining if the receiving client is qualified to receive the key based on a ticket previously obtained by the receiving client from a ticket server; and

transmitting the key from the key server to the receiving client if the receiving client is qualified;

wherein the request comprises one of a plurality of refresh requests, wherein each of the plurality of refresh requests corresponds to one of a plurality of forward security windows during the multicast event, wherein each of the plurality of forward security windows comprises a repeated time interval, and wherein receiving the refresh request comprises receiving the refresh request at a particular time within a corresponding forward

security window, said particular time being randomly generated by the receiving or sending client for a first forward security window and applied at the repeated time interval thereafter.

35. (New) A method comprising:

receiving a request for a key at a key server, said request being received from a receiving client, said key to facilitate access to a multicast event by the receiving client, wherein the key is a symmetric key that a sending client uses to encrypt the multicast event and the receiving client uses to decrypt the multicast event;

determining if the receiving client is qualified to receive the key based on a ticket previously obtained by the receiving client from a ticket server; and

transmitting the key from the key server to the receiving client if the receiving client is qualified;

wherein the key corresponds to a first interval of the multicast event, and wherein the method further comprises:

determining if the receiving client remains qualified to receive a refresh key; and

transmitting the refresh key to the receiving client if the receiving client remains qualified, said refresh key corresponding to the subsequent interval of the multicast event.

36. (New) A method comprising:

receiving a request for a key at a key server, said request being received from a receiving client, said key to facilitate access to a multicast event by the receiving client, wherein the key is a symmetric key that a sending client uses to encrypt the multicast event and the receiving client uses to decrypt the multicast event;

determining if the receiving client is qualified to receive the key based on a ticket previously obtained by the receiving client from a ticket server; and

transmitting the key from the key server to the receiving client if the receiving client is qualified;

wherein the key corresponds to a first interval of the multicast event, and wherein the method further comprises:

receiving a plurality of additional requests for the key from a plurality of additional receiving clients;

determining if each of the plurality of additional receiving clients are qualified to receive the key based on a ticket previously obtained by each of the plurality of additional receiving clients from the ticket server;

transmitting the key to each of the plurality of additional receiving clients that are qualified;

determining if the receiving client and each of the plurality of additional receiving clients remain qualified to receive a refresh key; and

transmitting the refresh key to the receiving client if the receiving client remains qualified and to each of the plurality of additional receiving clients that remain qualified, said refresh key corresponding to a subsequent interval of the multicast event.

37. (New) The method of claim 36 further comprising:

establishing a secure multicast link from the key server to the receiving client and the plurality of additional receiving clients, wherein the refresh key is transmitted through the secure multicast link.

38. (New) A method comprising:

receiving a request for a key at a key server, said request being received from a receiving client, said key to facilitate access to a multicast event by the receiving client, wherein the key is a symmetric key that a sending client uses to encrypt the multicast event and the receiving client uses to decrypt the multicast event;

determining if the receiving client is qualified to receive the key based on a ticket previously obtained by the receiving client from a ticket server; and

transmitting the key from the key server to the receiving client if the receiving client is qualified;

wherein the key server has a synchronized time with respect to the sending client for the event to within a margin of error, and wherein the method further comprises determining which of a plurality of available keys to use for said key based on the synchronized time.

39. (New) A machine readable storage medium having stored thereon machine executable instructions, the execution of said machine executable instructions to implement a method comprising:

receiving a request for a key at a key server, said request being received from a receiving client, and said key to facilitate an event between the receiving client and a sending client, wherein the key is a symmetric key that the sending client uses to encrypt the event and the receiving client uses to decrypt the event;

determining if the receiving client is qualified to receive the key based on a ticket previously obtained by the receiving client from a ticket server; and

transmitting the key from the key server to the receiving client if the receiving

client is qualified;

wherein the request comprises one of a plurality of refresh requests, wherein each of the plurality of refresh requests corresponds to one of a plurality of forward security windows during the event, wherein each of the plurality of forward security windows comprises a repeated time interval, and wherein receiving the refresh request comprises receiving the refresh request at a particular time within a corresponding forward security window, said particular time being randomly generated by the receiving or sending client for a first forward security window and applied at the repeated time interval thereafter.

40. (New) A machine readable storage medium having stored thereon machine executable instructions, the execution of said machine executable instructions to implement a method comprising:

receiving a request for a key at a key server, said request being received from a receiving client, and said key to facilitate an event between the receiving client and a sending client, wherein the key is a symmetric key that the sending client uses to encrypt the event and the receiving client uses to decrypt the event;

determining if the receiving client is qualified to receive the key based on a ticket previously obtained by the receiving client from a ticket server; and

transmitting the key from the key server to the receiving client if the receiving client is qualified;

wherein the key corresponds to a first interval of the event, and wherein the method further comprises:

receiving a plurality of additional requests for the key from a plurality of additional receiving clients;

determining if the each of the plurality of additional receiving

clients are qualified to receive the key based on a ticket previously obtained by each of the plurality of additional receiving clients from the ticket server;

transmitting the key to each of the plurality of additional receiving clients that are qualified;

determining if the receiving client and each of the plurality of additional receiving clients remain qualified to receive a refresh key; and

transmitting the refresh key to the receiving client if the receiving client remains qualified and to each of the plurality of additional receiving clients that remain qualified, said refresh key corresponding to a subsequent interval of the event.

41. (Previously Presented) The machine readable storage medium of claim 40 wherein the request is received within a predetermined time frame after the event starts, wherein said event is not encrypted during the predetermined period time frame.

42. (New) A method for facilitating a multicast of an event from a sending client to a plurality of receiving clients, the sending client multicasting event content to the receiving clients during an event interval having an event duration, the method comprising:

at a key server, sending a plurality of symmetric keys to each receiving client, each symmetric key being associated with a different time window within said event interval, each time window being of relatively short duration compared to the event duration, each symmetric key being used by the sending client to encrypt event content corresponding to said symmetric key's associated time window and being used by each receiving client to decrypt that resulting encrypted event content;

wherein, for each receiving client, each symmetric key is transmitted over a distinct

point-to-point link between the key server and that receiving client; and

wherein each symmetric key is transmitted to said plurality of receiving clients at randomly selected points in time prior to said symmetric key's associated time window, thereby promoting avoidance of undesirable traffic peaks at said key server.

43. (New) The method of claim 42, wherein said randomly selected points in time result from independent computations performed at each of said plurality of receiving clients.

44. (New) The method of claim 42, said event interval having a start time and including a first time window immediately following said start time, wherein said sending client does not encrypt the event content corresponding to said first time window, thereby promoting avoidance of an undesirable traffic peak at said key server just prior to said start time.

45. (New) The method of claim 42, wherein said time windows within said event interval are non-overlapping and are of substantially equal duration less than one-fourth of the event duration.

46. (New) The method of claim 42, wherein said event duration is continuous, wherein said time windows are of substantially equal duration on the order of one hour.

47. (New) The method of claim 42, said time windows being non-overlapping and of substantially equal duration, said event interval having a start time and including a first time window immediately following said start time, the method further comprising:

at the key server, receiving an initial key request from one of said receiving clients at an initial randomly selected point in time prior to said start time, said initial randomly selected point in time lying ahead of said start time by a first time difference;

sending a first symmetric key to said receiving client upon receipt of said initial key request, said first symmetric key corresponding to said first time window; and

for each subsequent time window, automatically sending the symmetric key associated with that subsequent time window to said receiving client without requiring further key requests from said receiving client, wherein said associated symmetric key is sent in advance of said subsequent time window by said first time difference.

48. (New) The method of claim 42, said time windows being non-overlapping and of substantially equal duration, said event interval having a start time and including a first time window immediately following said start time, the method further comprising:

at the key server, receiving an initial key request from one of said receiving clients at an initial randomly selected point in time prior to said start time;

sending a first symmetric key to said receiving client upon receipt of said initial key request, said first symmetric key corresponding to said first time window; and

for each subsequent time window, sending the symmetric key associated with that time window to said receiving client upon receiving a subsequent key request therefrom, wherein said subsequent key request is received at a random interval relative to other subsequent key requests for other subsequent time windows.